

Amendments to the Claims:

Claims 1-3, 5-14, 16-21, 23-33, and 35-50 were pending in this application. Please cancel all pending claims and insert therefor new claims 51-68 as follows:

1.-50. (canceled).

51. (new) A system for secure transmission of data over a public data transmission network, the system comprising:

a requesting computer connected to the network, the requesting computer requesting the secure transmission of data;

a server connected to the network, the server operative to encrypt the data requested by the requesting computer and transmit the encrypted data through the network;

a storage device associated with the requesting computer and connected to the network, the storage device operative to receive the encrypted data from the network, decrypt the received data, and store the decrypted data;

wherein the server directly contacts the storage device over the network to establish an encrypted data channel between the server and the storage device, the encrypted data channel excluding the requesting computer.

52. (new) The system as in claim 51 wherein the encrypted data channel comprises a secure sockets layer interface between the server and the storage device.

53. (new) The system as in claim 51 wherein the storage device sends a storage device public key to the server.

54. (new) The system as in claim 53 wherein the server sends a server public key to the storage device.

55. (new) The system as in claim 51 wherein the secure transmission of data comprises at least one of audio data and video data.

56. (new) The system as in claim 51 wherein the storage device stores the data in a removable medium.

57. (new) The system as in claim 56 wherein the removable medium is one of a compact disc (CD) and a digital versatile disc (DVD).

58. (new) The system as in claim 56 wherein the removable medium is one of a tape cartridge and a tape cassette.

59. (new) The system as in claim 56 wherein the removable medium is one of a holographic disc and a holographic cube.

60. (new) The system as in claim 51 wherein the storage device is a solid-state storage device.

61. (new) The system as in claim 51 wherein the storage device is independent of the requesting computer.

62. (new) A method for securely transmitting data from a server over a public data transmission network, the method comprising:

receiving a request from a client for transmission of requested data to a storage device directly connected to the network, the storage device associated with the client;

negotiating an encrypted communications channel with the storage device through the network, the encrypted communications channel excluding the client;

encrypting the requested data according to the negotiation with the storage device; and
sending the encrypted data to the storage device through the network.

63. (new) The method of claim 62 wherein negotiating an encrypted communications channel comprises establishing a secure sockets layer between the server and the storage device.

64. (new) The method of claim 62 wherein negotiating an encrypted communications channel comprises receiving a storage device public encryption key from the storage device.

65. (new) The method of claim 64 wherein negotiating an encrypted communications channel comprises sending a server public encryption key to the storage device.

66. (new) The method of claim 62 wherein negotiating an encrypted communications channel comprises receiving an encrypted master secret from the storage device.

67. (new) The method of claim 66 further comprising decrypting the master secret using a server private key, wherein the master secret is encrypted by the storage device using a server public key.

68. (new) The method of claim 66 wherein encrypting the requested data comprises encrypting the requested data based on the received master secret.